UNITED STATES DISTRICT COURT

ORIGINAL

for the

Central District of California

In the Matter of the Search of: Information associated with accounts identified as keno202@yahoo.com and others identified in Attachment A-1 that is within the possession, custody, or control of Yahoo! Inc.	)	Case No. 17MJ00477

FILED
2017 MAY 24 PM 2:53
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES
BY: AP

WARRANT PURSUANT TO 18 U.S.C. § 2703

To: Any Authorized Law Enforcement Officer

An application by a federal law enforcement officer requests the production and search of the following data:

See Attachment A-1

The data to be produced and searched, described above, are believed to contain the following:

See Attachment B-1

I find that the affidavit, or any recorded testimony, establishes probable cause to produce and search the data described in Attachment A-1, and to seize the data described in Attachment B-1. Such affidavit is incorporated herein by reference.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE HEREBY COMMANDED to serve this warrant on YAHOO! INC. in the daytime, between the hours of 6:00 a.m. and 10:00 p.m., within 14 days from the date of its issuance.

YAHOO! INC. IS HEREBY COMMANDED to produce the information described in Attachment A-1 within 10 calendar days of the date of service of this order. **YAHOO! INC. IS FURTHER COMMANDED** to comply with the further orders set forth in Attachment B-1, and shall not notify any person, including the subscriber(s) of the account/s identified in Attachment A-1, of the existence of this warrant.

The officer executing this warrant, or an officer present during the execution, shall prepare an inventory as required by law, and shall promptly return this warrant and the inventory to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE FURTHER COMMANDED to perform the search of the data provided by YAHOO! INC. pursuant to the procedures set forth in Attachment B-1.

Date and time issued: 3/6/17 2:35 p.m

Patrick J. Walsh
Judge's signature

City and State: Los Angeles, CA

Hon. Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Anil J. Antony, x6579 ASA

Return

Case No:	*Date and time warrant served on provider:*
17MJ00477	3/6/2017 at approx 6:05PM

Inventory made in the presence of: N/A (ISP warrant)

Inventory of data seized:
[Please provide a description of the information produced.]

DVD provided by Yahoo on 5/22/2017 via Fedex;
DVD labeled "338586" containing results for following accounts:

ask4dn, dnhovercraft2000, eseksno, Keno202, levifranco01, m-peters001, padarlingtonsmith, palmoliver3, thirdmainlandbridge, and related accounts

Certification

I declare under penalty of perjury that I am an officer involved in the execution of this warrant, and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: 5/24/2017

Executing officer's signature

RONALD J. MANUEL, SPECIAL AGENT

Printed name and title

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Yahoo! accounts identified as keno202@yahoo.com ("SUBJECT ACCOUNT #1"), padarlingtonsmith@yahoo.com ("SUBJECT ACCOUNT #2"), dnhovercraft2000@yahoo.com ("SUBJECT ACCOUNT #3"), eseksno@yahoo.com ("SUBJECT ACCOUNT #6"), m_peters001@yahoo.co.uk ("SUBJECT ACCOUNT #7"), thirdmainlandbridge@yahoo.com ("SUBJECT ACCOUNT #8"), levifranco01@yahoo.ca ("SUBJECT ACCOUNT #9"), and palmoliver3@yahoo.com ("SUBJECT ACCOUNT #10") that is within the possession, custody, or control of Yahoo! Inc., a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California 94089, regardless of where such information is stored, held, or maintained.

ATTACHMENT B-1

ITEMS TO BE SEIZED

I. SEARCH PROCEDURE

1. The search warrant will be presented to personnel of Yahoo! Inc. (the "PROVIDER" or "Yahoo!"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a. below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

5. If the search team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 120 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the content records beyond this 120-day period without first obtaining an extension of time order from the Court.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the PROVIDER (as applicable), including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A-1:

a. All contents of all wire and electronic communications associated with each SUBJECT ACCOUNT, limited to that which occurred on or after February 8, 2016 for SUBJECT ACCOUNTS #1 and #9; and since the inception of the account to the present for SUBJECT ACCOUNTS #2, #3, #6, #7, #8, and #10, including:

i. All emails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each email or message, and any related documents or attachments;

ii. All records or other information stored by subscriber(s) of the SUBJECT ACCOUNT, including address books, contact and buddy lists, calendar data, pictures or photos,

videos, notes, texts, links, user profiles, account settings, access logs, and files;

iii. All instant message ("IM") or chat communications associated with the SUBJECT ACCOUNT, including stored or preserved copies of the IMs sent to and from the accounts, private IMs, all chat logs in which one or more of the accounts were a participant (whether visibly or invisibly), private messages, transferred documents or files, buddy/friend/contact lists, pictures (whether displayed in chat or as icons/avatars of chat participants), as well as all metadata/IP/header information associated with any of the above;

iv. All websites and/or domain names associated with the SUBJECT ACCOUNT, including stored or preserved copies of files hosted on those sites or otherwise stored by those sites associated with the account;

v. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken;

vi. Any pictures, videos, or commentary written by the user of the SUBJECT ACCOUNT and all contributing viewers;

vii. All commands initiated by the SUBJECT ACCOUNT relating to features offered by the PROVIDER;

viii. All stored passwords, including passwords stored in clear text and hash form, and for any hashed values that include a salt, the PROVIDER shall provide the salt value used to compute the stored password hash value, and any security questions and answers;

ix. All search history and web history of the user of the SUBJECT ACCOUNT, including web clicks; and

x. All web browsing activities that are identifiable with the SUBJECT ACCOUNT.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or e-mail addresses associated with the account, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

(I) the SUBJECT ACCOUNTS;

(II) any other account associated with the cookie(s) associated with the SUBJECT ACCOUNTS;

(III) any other account associated with the SUBJECT ACCOUNT, including by means of sharing a common secondary, recovery, or alternate **e-mail address listed in subscriber records** for the SUBJECT ACCOUNT or by means of sharing a **common phone number or SMS number listed in subscriber records** for the SUBJECT ACCOUNT;

(IV) any other account accessed by a device with an identifier responsive to the device identifiers called for in paragraph 10.b.vi;

ii. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNTS described above in Section II.10.a, including but not limited to all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations;

iii. Any and all logs of user activity and user agent string, including: web requests or HTTP requests; any logs containing information such as the Requestor's IP address, identity and user ID, date and timestamp, request URI or URL, HTTP protocol version, referrer, and other user agent string information; login tracker logs; account management logs; and any other information concerning other email or social media

accounts accessed by or analytics related to the SUBJECT ACCOUNTS;

iv. Any and all cookies used by any computer or web browser associated with the SUBJECT ACCOUNTS, including the IP addresses dates and times associated with the recognition of any such cookie;

v. All subscriber information pertaining to any other account associated with the cookie(s) associated with each SUBJECT ACCOUNT, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or email addresses associated with the account including recovery/alternate email addresses, gender, date of birth, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records;

vi. Any information identifying the device or devices used to access any SUBJECT ACCOUNT, including any Android ID, Advertising ID, unique application number, hardware model, operating system version, unique device identifiers, Global Unique Identifier or "GUID," serial number, mobile network information, phone number, device serial number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"),

Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"), and any other information regarding the types of devices used to access each SUBJECT ACCOUNT or other device-specific information; and

vii. Any information showing the location of the user of each SUBJECT ACCOUNT, including while sending or receiving a message using a SUBJECT ACCOUNT or accessing or logged into a SUBJECT ACCOUNT.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For each SUBJECT ACCOUNT listed in Attachment A-1, as applicable, the search team may seize:

12. All information described above in Section II.10.a that constitutes evidence, contraband, fruits, or criminal violations of 18 U.S.C. § 371 (conspiracy); 18 U.S.C. § 1029(a)(2) (access device fraud); 18 U.S.C. §§ 1030(a)(2)(C) & (a)(4) (fraud and related activity in connection with computers); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1349 (conspiracy to commit wire fraud); and 18 U.S.C. § 1028A(a)(1) (aggravated identity theft) (collectively referred to as the "SUBJECT OFFENSES"), namely:

i. Information relating to who created, accessed, or used the SUBJECT ACCOUNT, including records about their identities and whereabouts.

ii. Evidence indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner or user.

iii. Information relating to a Business E-mail Compromise ("BEC") scheme, to include information relating to:

(I) the use of stolen or fraudulent identities to create, access, register, or use web domain or e-mail accounts;

(II) the compromise or spoofing of e-mail accounts, to include e-mail phishing;

(III) the use of e-mail to solicit a wire transfer;

(IV) the identification or selection of persons, businesses, or entities which may be accustomed to the sending of wire transfers;

(V) the identification or selection of persons with authority to request, initiate, or approve wire transfers;

(VI) the identification, acquisition, or use of persons or techniques used to move funds obtained via wire transfer, or other money laundering;

(VII) the location and/or the disposition of monies obtained via wire transfer;

(VIII) the discussion of shared criminal services, criminal web forums, or marketplaces offering criminal services where money mule, hacking, e-mail phishing, or laundering services might be obtained;

(IX) Look-alike/spoofed domains and/or associated legitimate domains they approximate;

(X) Potential victims of a BEC scheme;

(XI) Any Internet reconnaissance related to a BEC scheme or other fraudulent activity;

(XII) Fraudulent invoices or fake purchase orders;

(XIII) Any computer intrusion or email intrusion to monitor business transactions of potential victims of a BEC scheme;

(XIV) Online photos, online profiles, online resumes, or contact information of individuals identified for recruitment or use in a BEC scheme.

iv. Information relating to:

(I) The use or transmission of malware by the subject(s), including malware used to gain unauthorized access into computer systems, malware that functions as a keylogger, malware that takes screenshots of victims' computers, and malware that can be used to exfilatrate information from victims' computer systems;

(II) Documents or communications requesting Bitcoin and/or any other requests to transfer money or a monetary equivalent electronically;

(III) Communications between the SUBJECT ACCOUNT and other persons, accounts, coconspirators, or computers that involve the use of malware and/or unauthorized access to protected computers;

(IV) Victims, including Internet searches for information related to victim exploitation, the victims of computer intrusions, and/or the victims of malware;

(V) Internet accounts used for unauthorized access into computer systems and exploit attacks;

(VI) New account creations, or password resets;

(VII) Pictures or videos exchanged with victims or indicating the perpetrator of the scheme;

(VIII) Victim exploit tactics and possible new victims or other means of gaining access to victims' computer systems;

(IX) Computer programs or software that can be used to create, monitor, observe, or any other malicious software, or that can be used to obtain or secure unauthorized access to a computer or computer network, including the actual use, development, or operation of such programs or software; and

(X) Skills of the subject(s) related to computers used and their programing, coding, and engineering by the subject(s);

(XI) Possession, use, production, and/or trafficking of access devices, including credit and debit cards, or bank account information, in the names of the persons identified in the affidavit in support of this search warrant as KENNETH, DARLINGTON, and ESEKSNO.

(XII) Obtaining, possessing, using, or transferring personal and/or financial transaction identification information for persons other than the persons identified in the affidavit in support of this search warrant as KENNETH, DARLINGTON, and ESEKSNO, such as names, addresses, phone numbers, credit and debit card numbers, security codes, bank account and other financial institution account numbers, Social Security numbers, email addresses, Internet Protocol ("IP") addresses, as well as PIN numbers and passwords for financial institutions or internet service providers (collectively, "identity information");

(XIII) Data, records, or information reflecting or referencing purchases using unauthorized identity information;

(XIV) Documents or records containing personal identifying information for any individual that is not a person identified in the affidavit in support of this search warrant as KENNETH, DARLINGTON, and ESEKSNO, such as Social Security numbers, dates of birth, addresses, bank account numbers, driver's license numbers, and credit card numbers;

(XV) Any documents or records, including receipts, invoices, bank statements, and credit card statements,

evidencing the purchase of any products or services using altered, counterfeit, or fraudulent checks, access devices, or other monetary instruments;

(XVI) Data, records, or information relating to contacts or communications with co-conspirators engaged in the SUBJECT OFFENSES;

(XVII) Software, devices, or tools used to obtain, create, or use counterfeit or unauthorized checks or access devices such as credit, debit, bank, and gift cards;

(XVIII) Software or tools used to obtain, produce, utilize, organize or transfer of identity information;

(XIX) Communications or interactions with or among financial institutions such as banks, merchant processors, commercial payment services like PayPal, credit card companies, or investment companies;

(XX) Photographs of access devices or device-making equipment;

(XXI) Photographs of identity information for persons other than the persons identified in the affidavit in support of this search warrant as KENNETH, DARLINGTON, and ESEKSNO;

(XXII) The identity and location of the persons identified in the affidavit in support of this search warrant as KENNETH, DARLINGTON, and ESEKSNO, and any co-conspirators.

b. All records and information described above in Sections II.10.b.

IV. PROVIDER PROCEDURES

13. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

Special Agent Ronald J. Manuel
Federal Bureau of Investigation
11000 Wilshire Boulevard, Suite 1700
Los Angeles, California 90024
Tel.: 310-996-3553
Fax: 310-996-4458
Email: ronald.manuel@ic.fbi.gov

14. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

15. IT IS FURTHER ORDERED that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court or until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required.